CLAIMS

We claim:

1 A method for preventing unauthorized use of digital content data comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data; and

storing the modified data at predetermined memory locations.

2 The method of claim 1 wherein the digital data comprises data types selected from a group consisting of audio, video, documents, text and software.

3 The method of claim 1 wherein the data segments are of a variable length

4 The method of claim 1 wherein the second data comprises a randomly generated data stream.

5 The method of claim 1 wherein the second data comprises portions of the digital content data.

6 The method of claim 1 further comprising encrypting the modified data and storing the encrypted modified data.

7 The method of claim 6 further comprising encrypting the modified data with an encryption key.

8 The method of claim 7 further comprising encrypting the encryption key.

9 The method of claim 8 further comprising storing the encryption key with the encrypted modified data at the predetermined memory locations.

10 The method of claim 9 further comprising partitioning the encryption key among the encrypted modified data.

11 The method of claim 1 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

12 The method of claim 1 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored.

13 The method of claim 1 further comprising generating a map of locations at which the modified data is stored.

14 The method of claim 13 further comprising storing the map of locations at the predetermined memory locations.

15 The method of claim 1 wherein the memory locations reside on a system and further comprising:

scanning the system to determine available memory locations;

selecting target memory locations within the available memory locations at which to store the modified data; and

storing the modified data at the target memory locations.

16 The method of claim 15 wherein a subset of available memory locations are located within file system locations

17 The method of claim 15 wherein a subset of available memory locations are located outside file system locations.

18 The method of claim 15 further comprising generating a map of the target memory locations.

19 The method of claim 18 further comprising storing the map of target memory locations at the target memory locations.

20 The method of claim 1 further comprising:

retrieving the modified data from the predetermined memory locations; and

de-interleaving the data segments based on the second data to generate original digital content data.

21 The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

22 The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

23 The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

24 The method of claim 23 further comprising, if an authorized access of a file replaced by the modified data is determined, the file is accessed.

25 The method of claim 1 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data.

26 The method of claim 1 wherein modifying the data segments with second data comprises tokenizing the data segments with token data.

27 The method of claim 26 wherein the token data comprises lexical equivalents of assembly language commands.

28 The method of claim 27 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

29 A method for preventing unauthorized use of digital content data in a system having memory locations comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data;

scanning the system to determine available memory locations;

selecting target memory locations within the available memory locations at which to store the modified data; and

storing the modified data at the target memory locations.

30 The method of claim 29 wherein a subset of available memory locations are located within file system locations.

31 The method of claim 29 wherein a subset of available memory locations are located outside file system locations.

32 The method of claim 29 further comprising generating a map of the target memory locations.

33 The method of claim 32 further comprising storing the map of target memory locations at the target memory locations.

34 The method of claim 29 wherein the digital data comprises data types selected from a group consisting of audio, video, documents, text and software.

35 The method of claim 29 wherein the data segments are of a variable length

36 The method of claim 29 wherein the second data comprises a randomly generated data stream.

37 The method of claim 29 wherein the second data comprises portions of the digital content data.

38 The method of claim 29 further comprising encrypting the modified data and storing the encrypted modified data.

39 The method of claim 38 further comprising encrypting the modified data with an encryption key.

40 The method of claim 39 further comprising encrypting the encryption key.

41 The method of claim 40 further comprising storing the encryption key with the encrypted modified data at the predetermined memory locations.

42 The method of claim 41 further comprising partitioning the encryption key among the encrypted modified data.

43 The method of claim 29 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

44 The method of claim 29 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored.

45 The method of claim 29 further comprising generating a map of locations at which the modified data is stored.

46 The method of claim 45 further comprising storing the map of locations at the predetermined memory locations.

47 The method of claim 29 further comprising:

retrieving the modified data from the predetermined memory locations; and

de-interleaving the data segments based on the second data to generate original digital content data.

48 The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

49 The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

50 The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

51 The method of claim 50 further comprising, if an authorized access of a file replaced by the modified data is determined, the file is accessed.

52 The method of claim 29 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data.

53 The method of claim 29 wherein modifying the data segments with second data comprises tokenizing the data segments with token data.

54 The method of claim 53 wherein the token data comprises lexical equivalents of assembly language commands.

55 The method of claim 54 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data to deter unauthorized access.

56 A method for preventing unauthorized use of digital content data hosted on a system comprising:

modifying the digital content data with saturation data to generate modified data; and

storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data.

57 The method of claim 56 further comprising subdividing the digital content data into data segments and modifying the data segments.

58 The method of claim 56 further comprising:

determining whether an unauthorized attempt at accessing the digital content data occurs;

in the event of unauthorized access, generating saturation traffic on the system to deter the unauthorized activity.

59 The method of claim 58 wherein the saturation traffic comprises system commands that burden system resources.

60 The method of claim 59 wherein the system commands are generated as a function of activity utilizing the system resources subject to the unauthorized access.

61 The method of claim 58 wherein determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted.

62 The method of claim 56 further comprising interleaving the digital content data with second data to generate interleaved data.

63 The method of claim 56 further comprising tokenizing the digital content data with token data.

64 A method for preventing unauthorized use of digital content data hosted on a system wherein a table of contents identifies files stored at memory locations of the system comprising:

identifying at the table of contents a first memory location referring to a location at which at which first data file is stored;

modifying the first memory location in the table of contents to refer to a second data file at a second location; and

upon an attempt at access by the system of the first data file, accessing the second data file if the attempt is unauthorized.

65 The method of claim 64 further comprising accessing the first data file if the attempt is authorized.

66 A method for preventing unauthorized use of digital content data hosted on a system wherein a table of contents identifies files stored at memory locations of the system comprising:

identifying at the table of contents a first memory location referring to a location at which at which first data file is stored;

copying the contents of the first data file to a second memory location; and

replacing the first data file with a second data file;

upon an attempt at access by the system of the first data file, accessing the second data file if the attempt is unauthorized.

67 The method of claim 66 further comprising accessing the first data file if the attempt is authorized.

68 A method for preventing unauthorized use of digital content data hosted on a system comprising:

monitoring an operating system interface of the system to determine access of operating system resources; and

repeatedly generating a shim on the operating system interface to deter unauthorized access of the digital content data.

69 The method of claim 68 wherein the shim is generated in the event of an unauthorized access.

70 The method of claim 68 wherein the shim is repeatedly generated periodically, each shim being regenerated following a predetermined time period.

71 The method of claim 68 wherein the shim comprises first and second shims generated on the operating system interface for operation in front of and behind the unauthorized access respectively.

72 The method of claim 68 wherein generating the shim comprises initiating an operation that generates saturation data.

73 A method for preventing unauthorized use of digital content data hosted on a system comprising:

substituting a portion of the digital content data with token data to generate tokenized data; and

storing the tokenized data at predetermined memory locations on the system to deter unauthorized access of the digital content data.

74 The method of claim 73 further comprising subdividing the digital content data into data segments and substituting a portion of the data segments.

75 The method of claim 73 further comprising interleaving the digital content data with second data to generate interleaved digital content data.

76 The method of claim 75 further comprising:

determining whether an unauthorized attempt at accessing the digital content data occurs;

in the event of unauthorized access, generating saturation traffic on the system to deter the unauthorized activity.

77 The method of claim 76 wherein the saturation traffic comprises system commands that burden system resources.

78 The method of claim 73 wherein the token data comprises lexical equivalents of assembly language commands.

79 The method of claim 78 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data to deter unauthorized access thereof.

80 A method for preventing unauthorized use of digital content data hosted on a system comprising:

monitoring an operating system interface operating on the system and the digital content data at an assassin process to determine whether an unauthorized attempt at accessing the digital content data occurs; and

in the event of unauthorized access, deterring the unauthorized access and communicating the unauthorized access to the operating system interface.

81 The method of claim 80 wherein the assassin process further determines whether secondary assassin processes are located on the operating system interface, and, if so, causes the secondary assassin processes to exit.

82 The method of claim 80 wherein deterring unauthorized access comprises generating saturation data to deter the unauthorized activity.

83 The method of claim 80 wherein the step of monitoring comprises assembling a list of authorized accesses and comparing a newly generated process with the list to determine a status of the newly generated process as being authorized or unauthorized.

84 The method of claim 83 wherein the step of monitoring further tracks descendant processes of processes on the list to determine the status of the descendant process.

85 A method for preventing unauthorized use of digital content data in a system having memory locations comprising:

scanning the system to determine available memory locations based on a file system identifying locations of files on the system;

selecting target memory locations within the available memory locations at which to store the digital content data; and

storing the digital content data at the target memory locations.

86 The method of claim 85 wherein a subset of available memory locations are located within files identified by the file system locations.

87 The method of claim 85 wherein a subset of available memory locations are located between files identified by the file system locations.

88 The method of claim 85 wherein a subset of available memory locations are located outside the file system locations.

89 A system for preventing unauthorized use of digital content data comprising:

a subdividing unit for subdividing the digital content data into data segments;

a modification unit for modifying the data segments with second data to generate modified data; and

a storage unit for storing the modified data at predetermined memory locations.

90 The system of claim 89 wherein the data segments are of a variable length

91 The system of claim 89 wherein the second data comprises a randomly generated data stream.

92 The system of claim 89 wherein the second data comprises portions of the digital content data.

93 The system of claim 89 further comprising an encryption unit for encrypting the modified data and storing the encrypted modified data.

94 The system of claim 93 wherein the encryption unit further encrypts the modified data with an encryption key.

95 The system of claim 94 wherein the encryption unit further encrypts the encryption key.

96 The system of claim 95 wherein the storage unit further stores the encryption key with the encrypted modified data at the predetermined memory locations.

97 The system of claim 96 further comprising a partitioning unit for partitioning the encryption key among the encrypted modified data.

98 The system of claim 89 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

99 The system of claim 89 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored.

100 The system of claim 89 further comprising a map generator for generating a map of locations at which the modified data is stored.

101 The system of claim 100 wherein the storage unit further stores the map of locations at the predetermined memory locations.

102 The system of claim 89 wherein the memory locations reside on the system and further comprising:

a scanner for scanning the system to determine available memory locations;

a selector for selecting target memory locations within the available memory locations at which to store the modified data; and

wherein the storage unit stores the modified data at the target memory locations.

103 The system of claim 102 wherein a subset of available memory locations are located within file system locations

104 The system of claim 102 wherein a subset of available memory locations are located outside file system locations.

105 The system of claim 102 further comprising a map generator for generating a map of the target memory locations.

106 The system of claim 105 wherein the storage unit stores the map of target memory locations at the target memory locations.

107 The system of claim 89 further comprising:

means for retrieving the modified data from the predetermined memory locations; and

means for de-interleaving the data segments based on the second data to generate original digital content data.

108 The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

109 The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

110 The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

111 The system of claim 89 wherein the modification unit modifies the data segments comprises interleaving the data segments with the second data to generate interleaved data.

112 The system of claim 89 wherein the modification unit modifies the data segments with second data comprises tokenizing the data segments with token data.

113 The system of claim 112 wherein the token data comprises lexical equivalents of assembly language commands.

114 The system of claim 113 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

115 A system for preventing unauthorized use of digital content data in a system having memory locations comprising:

means for subdividing the digital content data into data segments;

means for modifying the data segments with second data to generate modified data;

means for scanning the system to determine available memory locations;

a selector for selecting target memory locations within the available memory locations at which to store the modified data; and

a storage unit for storing the modified data at the target memory locations.

116 The system of claim 115 wherein a subset of available memory locations are located within file system locations.

117 The system of claim 115 wherein a subset of available memory locations are located outside file system locations.

118 The system of claim 115 further comprising a map generator for generating a map of the target memory locations.

119 The system of claim 118 wherein the storage unit stores the map of target memory locations at the target memory locations.

120 The system of claim 115 further comprising means for encrypting the modified data and wherein the storage unit stores the encrypted modified data.

121 The system of claim 120 wherein the means for encrypting further encrypts the modified data with an encryption key.

122 The system of claim 121 wherein the means for encrypting further encrypts the encryption key.

123 The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

124 The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

125 The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

126 A system for preventing unauthorized use of digital content data hosted on a system comprising:

a modification unit for modifying the digital content data with saturation data to generate modified data; and

a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data.

127 The system of claim 126 further comprising subdividing the digital content data into data segments and modifying the data segments.

128 The system of claim 126 further comprising means for determining whether an unauthorized attempt at accessing the digital content data occurs, and, in the event of unauthorized access, means for generating saturation traffic on the system to deter the unauthorized activity.

129 The system of claim 128 wherein the saturation traffic comprises system commands that burden system resources.

130 The system of claim 129 wherein the system commands are generated as a function of activity utilizing the system resources subject to the unauthorized access.

131 The system of claim 128 wherein the means for determining whether an unauthorized attempt at accessing the digital content data occurs monitors activity of the system hosting the digital content data and determines whether the activity is inconsistent with the type of digital content data being hosted.

132 The system of claim 126 further comprising means for interleaving the digital content data with second data to generate interleaved data.

133 The system of claim 126 further comprising means for tokenizing the digital content data with token data.

134 A system for preventing unauthorized use of digital content data hosted on a system wherein a table of contents identifies files stored at memory locations of the system comprising:

a table of contents for identifying a first memory location referring to a location at which at which first data file is stored;

a modification unit for modifying the first memory location in the table of contents to refer to a second data file at a second location; and

access means for, upon an attempt at access by the system of the first data file, accessing the second data file if the attempt is unauthorized.

135 The system of claim 134 wherein the access means further accesses the first data file if the attempt is authorized.

136 A system for preventing unauthorized use of digital content data hosted on a system wherein a table of contents identifies files stored at memory locations of the system comprising:

a table of contents for identifying a first memory location referring to a location at which at which first data file is stored;

means for copying the contents of the first data file to a second memory location; and

means for replacing the first data file with a second data file;

access means for, upon an attempt at access by the system of the first data file, accessing the second data file if the attempt is unauthorized.

137 The system of claim 136 wherein the access means accesses the first data file if the attempt is authorized.

138 A system for preventing unauthorized use of digital content data hosted on a system comprising:

means for monitoring an operating system interface of the system to determine access of operating system resources; and

means for repeatedly generating a shim on the operating system interface to deter unauthorized access of the digital content data.

139 The system of claim 138 wherein the shim is generated in the event of an unauthorized access.

140 The system of claim 138 wherein the shim is repeatedly generated periodically, each shim being regenerated following a predetermined time period.

141 The system of claim 138 wherein the shim comprises first and second shims generated on the operating system interface for operation in front of and behind the unauthorized access respectively.

142 The system of claim 138 wherein the means for generating the shim further initiates an operation that generates saturation data.

143 A system for preventing unauthorized use of digital content data hosted on a system comprising:

means for substituting a portion of the digital content data with token data to generate tokenized data; and

means for storing the tokenized data at predetermined memory locations on the system to deter unauthorized access of the digital content data.

144 The system of claim 143 further comprising means for subdividing the digital content data into data segments and substituting a portion of the data segments.

145 The system of claim 143 further comprising means for interleaving the digital content data with second data to generate interleaved digital content data.

146 The system of claim 143 further comprising:

means for determining whether an unauthorized attempt at accessing the digital content data occurs; and

means for generating saturation traffic on the system to deter the unauthorized activity in the event of unauthorized access.

147 The system of claim 146 wherein the saturation traffic comprises system commands that burden system resources.

148 The system of claim 143 wherein the token data comprises lexical equivalents of assembly language commands.

149 The system of claim 148 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data to deter unauthorized access thereof.

150 A system for preventing unauthorized use of digital content data hosted on a system comprising:

an assassin process for monitoring an operating system interface operating on the system and the digital content data to determine whether an unauthorized attempt at accessing the digital content data occurs; and

means for deterring the unauthorized access and communicating the unauthorized access to the operating system interface, in the event of unauthorized access.

151 The system of claim 150 wherein the assassin process further determines whether secondary assassin processes are located on the operating system interface, and, if so, causes the secondary assassin processes to exit.

152 The system of claim 150 wherein the means for deterring unauthorized access comprises means for generating saturation data to deter the unauthorized activity.

153 The system of claim 150 wherein the assassin process assembles a list of authorized accesses and compares a newly generated process with the list to determine a status of the newly generated process as being authorized or unauthorized.

154 The system of claim 153 wherein the assassin process further tracks descendant processes of processes on the list to determine the status of the descendant process.

155 A system for preventing unauthorized use of digital content data in a system having memory locations comprising:

a scanner for scanning the system to determine available memory locations based on a file system identifying locations of files on the system;

means for selecting target memory locations within the available memory locations at which to store the digital content data; and

a storage unit for storing the digital content data at the target memory locations.

156 The system of claim 155 wherein a subset of available memory locations are located within files identified by the file system locations.

157 The system of claim 155 wherein a subset of available memory locations are located between files identified by the file system locations.

158 The system of claim 155 wherein a subset of available memory locations are located outside the file system locations.

159 A system for preventing unauthorized use of digital content data in a system having memory locations wherein the system enables a user to select from a plurality of tool modules, each module providing a service for protecting digital content from unauthorized use such that a user can protect digital content.

160 The system of claim 159 wherein the tool modules comprise modules that perform functions selected from the group of functions consisting of: interleaving; tokenization; obfuscation; saturation; translocation; shimming and assassination.